Lösungsblatt – WLAN Arbeitsblatt

◇ Teil 1: Lückentext

WLAN steht für **Wireless Local Area Network** und beschreibt ein drahtloses **lokales** Netzwerk.

Es ermöglicht die Verbindung von Geräten wie **Smartphones**, **Laptops** und **Tablets** ohne Kabel.

Ein WLAN besteht aus einem sogenannten **Access Point**, der als zentrale Funkstation dient, und mehreren **Clients/Endgeräten**, die sich mit diesem verbinden.

Die Datenübertragung erfolgt über elektromagnetische **Funkwellen** im Frequenzbereich von **2,4** GHz und **5 (6)** GHz.

Im Gegensatz zu kabelgebundenen Netzwerken ist WLAN ein sogenanntes **Shared Medium**. Das bedeutet, dass sich mehrere Geräte die verfügbare **Bandbreite** teilen müssen.

Außerdem arbeitet WLAN im **Half-Duplex**-Modus, was bedeutet, dass ein Gerät entweder senden oder empfangen kann, aber nicht beides gleichzeitig.

Typische Störungen entstehen durch **andere WLAN-Netze**, **Wände/Hindernisse** und andere Funkquellen wie **Bluetooth oder Mikrowellen**.

◇ Teil 2: Verständnis & Technik

1. Warum ist WLAN langsamer als LAN?

- Shared Medium → Bandbreite wird geteilt
- Half-Duplex → kein gleichzeitiges Senden/Empfangen
- Störungen und Interferenzen

2. Was bedeutet „Shared Medium“ im WLAN?
Mehrere Geräte nutzen denselben Übertragungskanal → nur ein Gerät kann gleichzeitig senden.

3. Unterschied Half-Duplex / Full-Duplex

- Half-Duplex: Senden ODER Empfangen gleichzeitig (WLAN)
- Full-Duplex: Senden UND Empfangen gleichzeitig (LAN)

4. Warum sind Kanäle 1, 6 und 11 wichtig?
Weil sie sich im 2,4 GHz Band **nicht überlappen** → weniger Störungen.

5. Vorteile/Nachteile 5 GHz vs 2,4 GHz

Vorteile:

- höhere Datenrate
- weniger Störungen

Nachteile:

- geringere Reichweite
- schlechtere Durchdringung von Wänden

◇ Teil 3: Sicherheit

6. Gefahren in öffentlichen WLANs

- Abhören von Daten
- Fake Hotspots
- Malware / Phishing

7. Man-in-the-Middle Angriff

Ein Angreifer schaltet sich zwischen Nutzer und Netzwerk und kann Daten **mitlesen oder manipulieren**.

8. Warum sind offene WLANs gefährlich?

- keine Verschlüsselung
- Daten können im Klartext übertragen werden
- Angreifer können leicht mithören

9. Was ist ein VPN und wie schützt es?

Ein VPN (Virtual Private Network) verschlüsselt die gesamte Verbindung und schützt Daten vor Mitlesen im Netzwerk.

10. Warum ersetzt ein VPN kein sicheres Verhalten?

- Phishing weiterhin möglich
- unsichere Webseiten bleiben gefährlich
- Nutzer kann trotzdem Daten preisgeben